





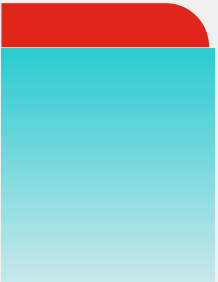
FORTINET[®]

資安SIEM境遇 - Fortinet讓校園 擁有毫不妥協的安全防護

Jarvis Lee 李尚峰

Fortinet 台灣區技術顧問

lj Jarvis@fortinet.com



現今資安與網維面臨的挑戰

不僅需要防護型資安解決方案，還需要建立早期預警系統



太多供應商
資訊難統整



大量日誌與告警
關聯分析困難



手動回應緩慢
費工耗時易出錯



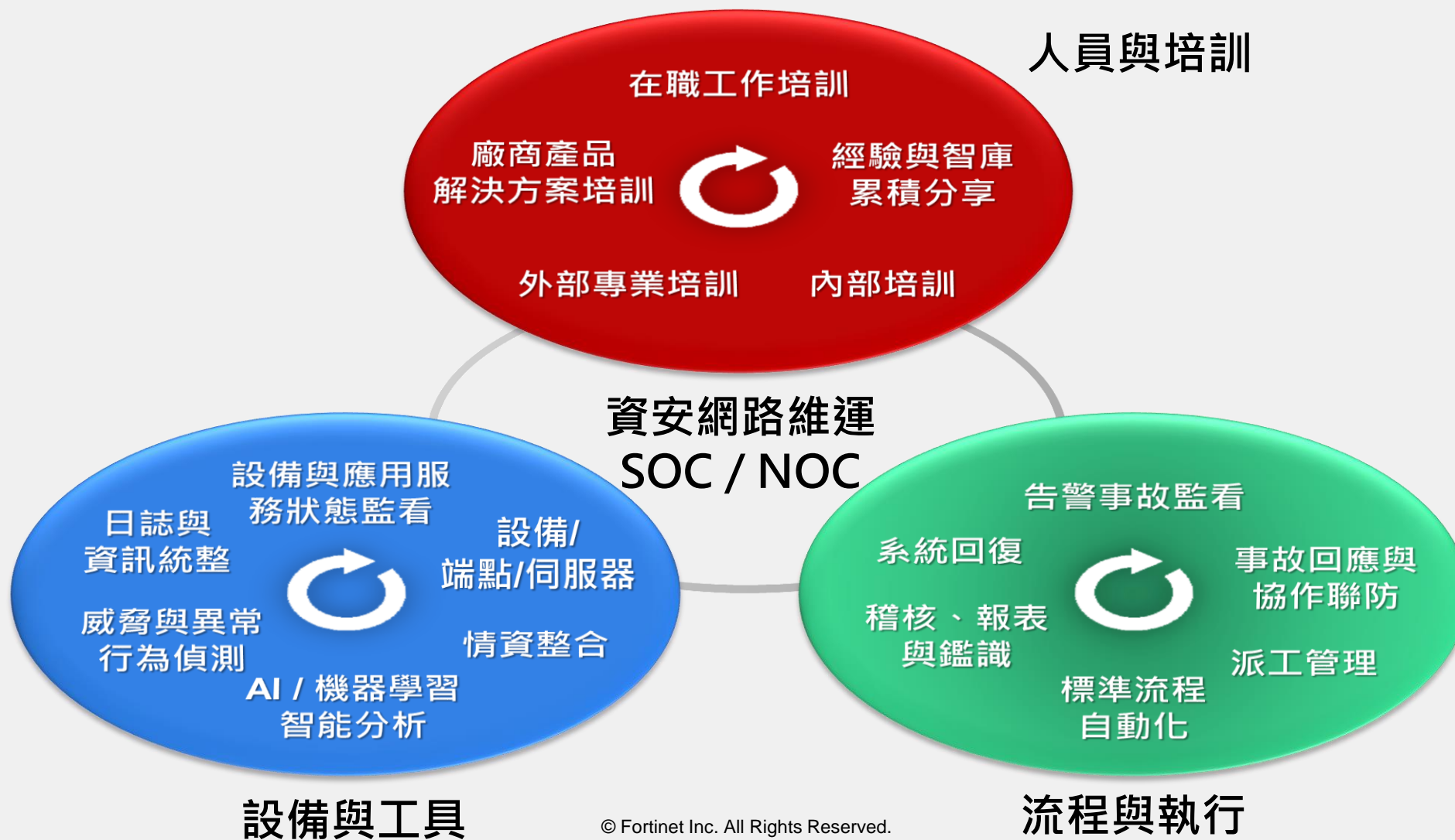
缺乏有經驗
的人員



管理複雜導致
高維運成本

資安網維控管三重奏

導入好的設備與解決方案、簡單易用、標準化作業流程



導入 AI 與機器學習，加速進階威脅偵測

AI 驅動的安全防護深入產品 DNA

基於網路資訊流 Network-Based



FortiSandbox



FortiNDR
(aka FortiAI)

基於日誌與記錄 Log-Based



FortiSIEM

基於終端行為模式 Endpoint-Based



FortiEDR



FortiGuard Lab.
Global Threat Intelligence Services

基於資安情資服務 TIS-Based

© Fortinet Inc. All Rights Reserved.

FortiSIEM 您維運管理的好幫手

資料統整、威脅偵測、維運監看、事故回應一氣呵成

標準化事故回應作業流程

- 內建派工管理系統，方便告警事故通報、分流、追蹤和管理告警事故調查與回應

告警事故協作聯防自動化

- 使用預或自定義的緩解調控腳本，手動或自動回應告警事故

豐富彈性的監看儀表板與報表

- 有效增進系統運作效能、可用度與資安可視性，滿足監管稽核需求

直覺式事件關聯分析，簡單易用

- Google-like 的快速資料查找方式搭配選單點擊，無需學習複雜的查詢語法

多來源、多品牌日誌記錄統整與加值

- 融合 SOC 與 NOC，日誌、流量、效能資訊、應用服務記錄統整與內容加值

設備組態管理資料庫 (CMDB)

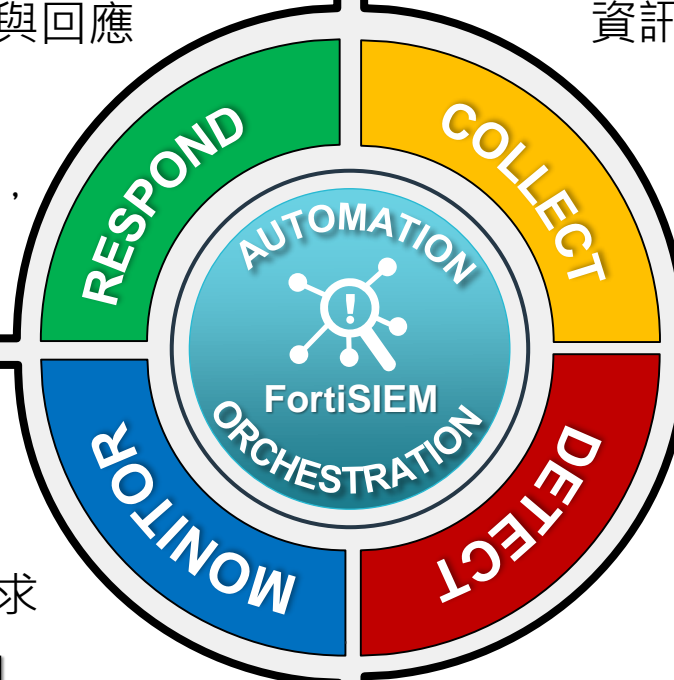
- 監看管理設備效能指標和組態
- 設備資產統整、威脅情資整合

智能分析 (AI)，機器學習 (ML)

- 快速學習建立維運維運基準線
- 即時偵測異常行為與潛在威脅

對應 MITRE ATT&CK 資安框架

- 提供威脅情境定性分析，有效偵測進階持續性威脅 (APT)



資安 (SOC) 與網維 (NOC) 融合式分析

完善您整體資安與網維的可視性

資安日誌與資訊

NGFW / IPS / VPN

EPP/EDR

Web Application

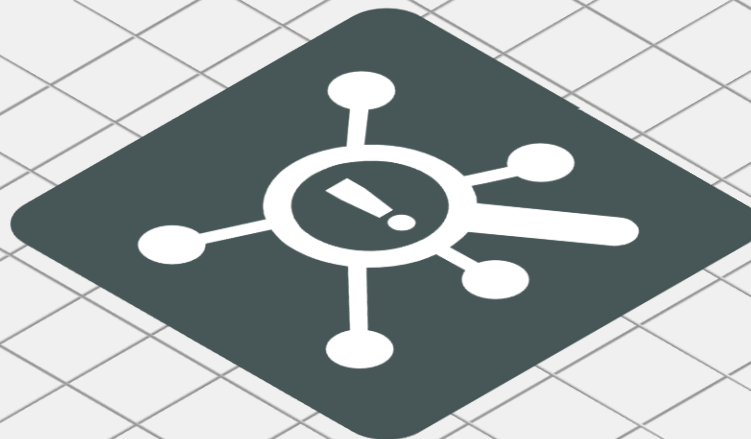
eMail System

AAA Server

Database

Traffic / Flows

Router / Switch / WLAN, etc.



設備效能監看指標

CPU

Memory

Storage

Interface Utilization

Uptime

Process / Services

Configuration, etc.

融合式的資安與網維管理 (SOC & NOC)

更多豐富的功能 | 更好的可視性 | 加速事故回應時間



智能分析 (AI) 與 機器學習 (ML) 關聯規則

1500+

預設智能關聯分析規則，橫跨四大領域：

- 資安 (Security)
- 效能 (Performance)
- 可用度 (Availability)
- 異動 (Change)

可自行定義修改關聯分析規則來
滿足各種監看告警需求

Performance

Availability

System

Application

Network

Application

Network

Server

Storage

Server

Environmental

Storage

Change

Beaconing

Server

Network

Beaconing

Security

Exploits

Authentication

Vulnerabilities

Policy Violation

Behavior Anomaly

Airline
Security

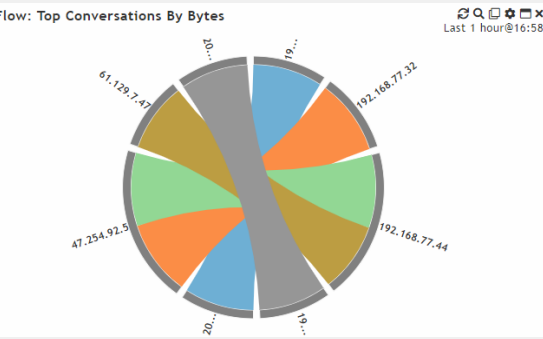


內建豐富稽核與 合規性報表

3000+

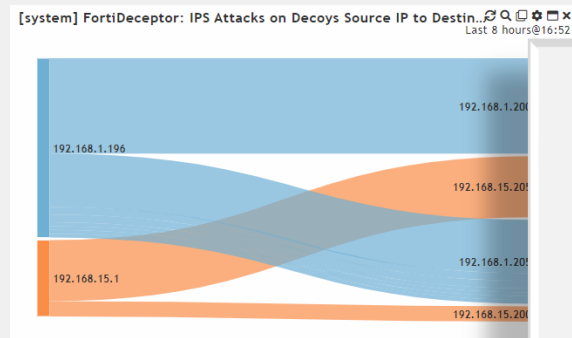
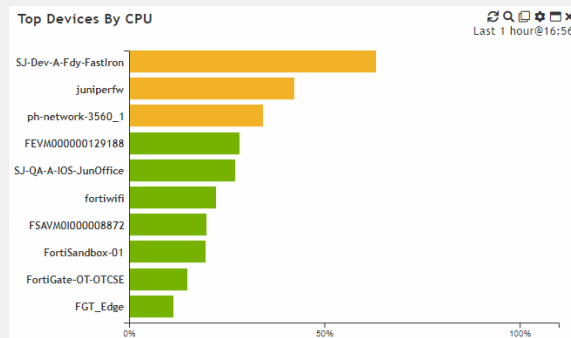
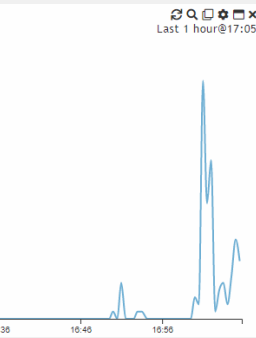
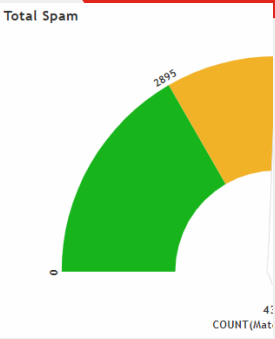
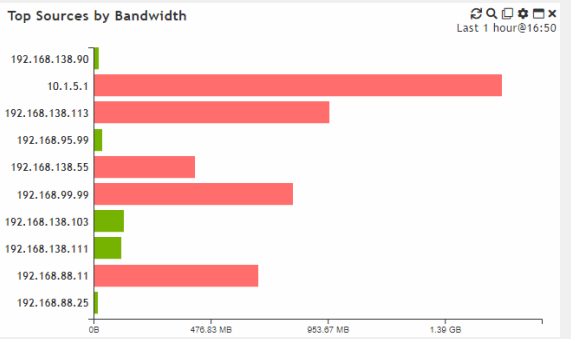
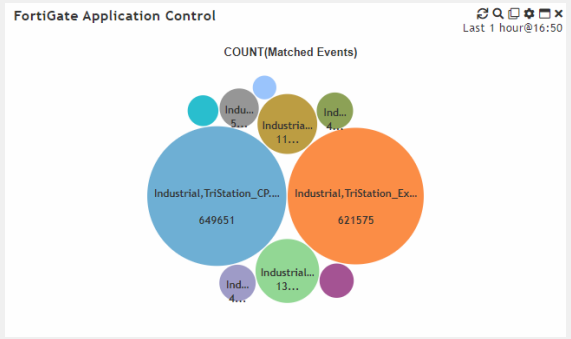
預設合規性報表 (Compliance Reports) :
包括 PCI, SOX, HIPAA, FISMA, NERC,
COBIT, ITIL, NIST, ISO, GLBA, GPG13,
CIS, SANS, Critical Controls

內建報表客製化建構器 :
3,000+ 可客製化欄位，豐富的圖表
資源庫，可穿插文字與附件



Top Malware

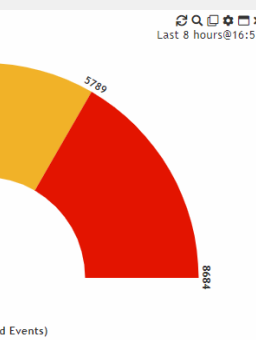
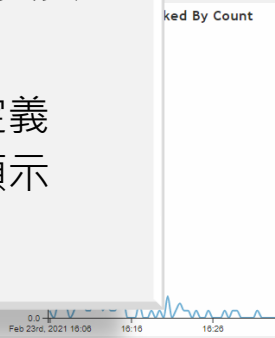
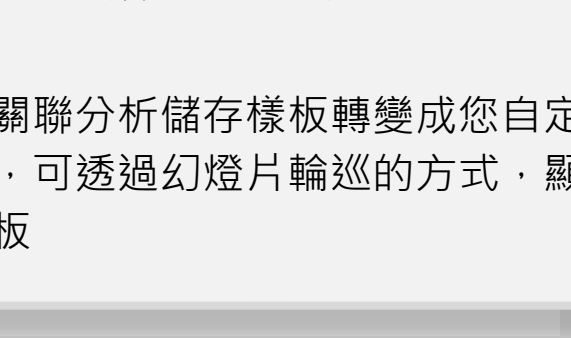
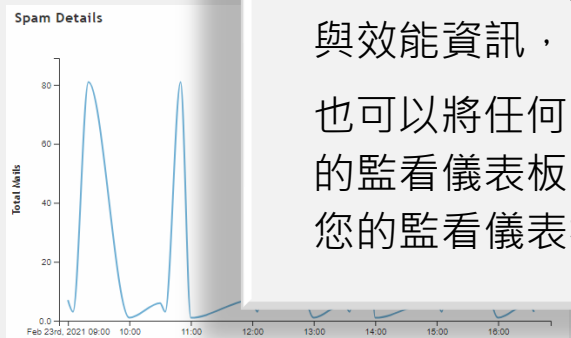
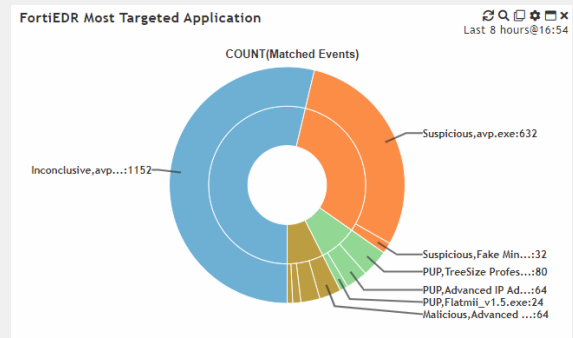
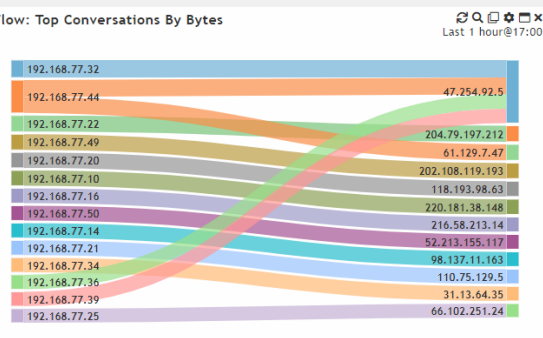
Malware	Source	Destination	Count
W32/Amadey.94...	10.1.0.18	45.141.84.184	144
MSIL/Kryptik.GV...	10.1.0.13	202.28.49.85	16
MSIL/Kryptik.GV...	10.1.0.19	202.28.49.85	16
PossibleThreat...	10.1.0.18	195.22.153.244	16
PossibleThreat.P...	10.1.0.18	217.160.0.230	16
VBA/Agent.LAG!...	10.100.91.5	10.100.66.200	16
W32/BitCoinMin...	10.1.0.12	210.153.27.14	16
W32/Crypren.AF...	10.100.91.11	10.100.66.11	16



任何關聯分析結果都可變成您的儀表板

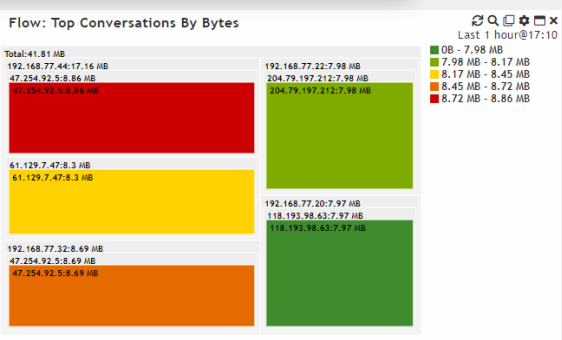
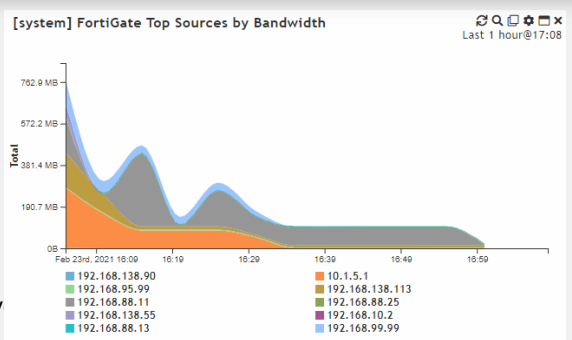
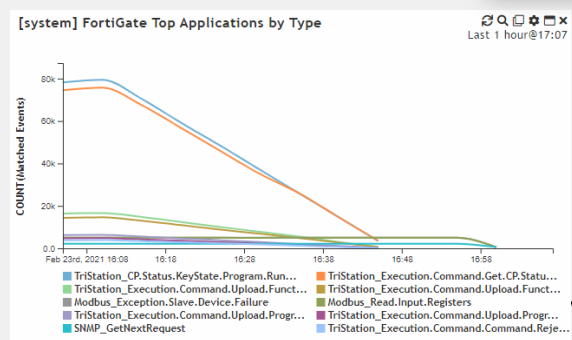
FortiSIEM 提供眾多預設的儀表板方便您監看資安與效能資訊，

也可以將任何關聯分析儲存樣板轉變成您自定義的監看儀表板，可透過幻燈片輪巡的方式，顯示您的監看儀表板



OT - Incidents in Purdue Levels - Security Incidents Summary

Event Name	Severity Category	Purdue Level	Total Unique Incidents
Sudden Increase in DNS Requ...	MEDIUM	Level 3.5	2
Large Outbound Transfer	MEDIUM	Level 2	2
Large Outbound Transfer	MEDIUM	Level 3.5	2
Large Outbound Transfer To O...	MEDIUM	Level 3.5	2
Sudden Increase in DNS Requ...	MEDIUM	Level 2	1
Sudden Increase in Firewall C...	MEDIUM	Level 3.5	1
Sudden Increase in Reported ...	MEDIUM	Level 3.5	1
Sudden Increase in Traffic Fr...	MEDIUM	Level 2	1
Sudden Increase in Traffic Fr...	MEDIUM	Level 3.5	1
Executive End User DNS Quer...	MEDIUM	Level 3.5	1



資料統整

Collect



應用範例一：設備識別與資料統整

Collect

排程自動探索環境，身分、設備與連網位置自動關聯

- 透過排程自動探索環境 (ping only discovery)，更新 CMDB 資料庫，產生“Unmanaged”狀態日報表，偵測非納管設備

The screenshot displays the FortiSIEM CMDB interface. At the top, there is a navigation bar with various icons and labels: 儀表板, 關聯分析, 告警事故, 派工管理, CMDB, 資源庫, 工作, 系統管理. Below this, a summary row shows counts for different device types: Routers (4), Firewalls (15), Windows (1), Unix (4), ESX (0), AWS (0), Azure (0), and OT/IoT (0). The main content area is titled 'CMDB > Devices' and features a table of devices. The table has columns for Name, IP, Device Type, Status, Method, Organization, Agent Policy, Agent Status, and Monitoring Status. A single device is listed with the name 'HOST-10.1.217.1', IP '10.1.217.1', Device Type 'Generic', and Status 'Unmanaged'. The 'Unmanaged' status is highlighted with a red box. The interface also includes a sidebar on the left with navigation options like Devices, Applications, Users, Business Services, and CMDB Reports. At the bottom, there are tabs for Summary, Attributes, Monitoring, Software, Hardware, Configuration, Correlation, and Archives, along with an '自動展開' (Auto-expand) checkbox.

名稱	IP	設備型式	狀態	方法	組織	代理程式政策	代理程式狀態	監看狀態
HOST-10.1.217.1	10.1.217.1	Generic	Unmanaged	PING	Super			

應用範例二：設備識別與資料統整

Collect

排程自動探索環境，身分、設備與連網位置自動關聯

- 透過排程自動探索環境 (L2 Scan)，更新“Identity & Location”儀表板，方便識別人員、設備與連線位置

The screenshot shows the 'Identity & Location' dashboard interface. Four red callout boxes with arrows point to specific data sources: '來自 DHCP 日誌' (from DHCP logs) points to the IP and MAC columns; '來自 AD 登入日誌' (from AD login logs) points to the User and Host Name columns; '來自 L2 交換器 自動探索記錄' (from L2 switch auto-discovery records) points to the VLAN ID and Connected to columns; and '來自所有相關 日誌或記錄' (from all related logs or records) points to the First Seen and Last Seen columns. A table of data is displayed below, with the second row highlighted in red.

IP Address	MAC Address	User	Host Name	Domain	VLAN ID	Connected to	First Seen	Last Seen
192.168.26.120	00:26:b9:1f:3b:76	sara.tanner (Domain)	stanner-laptop	ACCELOPS			Jun 24, 2021 1:58:41 AM	Jul 9, 2021 1:55:11 AM
192.168.64.187	00:0c:29:9d:d4:c6	svc_monitor (Domain)	lab03-ws145Cw8-2	ACCELOPS	22	ph-network-3560_1 192.168.19.1 (GigabitEthernet0/14)	Jun 24, 2021 1:23:52 AM	Jul 9, 2021 1:56:08 AM
192.168.20.116	00:0c:29:4e:e1:e8	svc_monitor (Domain)	lab03-ws145Cw8	ACCELOPS	30	SJ-Main-Cat6500 192.168.20.1 (GigabitEthernet1/36)	Jun 24, 2021 1:23:52 AM	Jul 9, 2021 1:56:18 AM
192.168.20.157	f0:4d:a2:96:b6:f9	jeff.price (Domain)	jprice-desktop	ACCELOPS	5	SJ-Main-Cat6500 192.168.20.1 (GigabitEthernet0/19)	Jul 8, 2021 9:00:42 PM	Jul 9, 2021 1:33:33 AM
192.168.26.119	c0:cb:38:15:97:e5	jeff.price (Domain)	jprice-laptop	ACCELOPS			Jul 7, 2021 9:00:02 AM	Jul 9, 2021 1:43:07 AM
192.168.26.102	00:23:5a:3e:62:69	jared.anderson (Domain)	lab02-ws075Cw8-LAPTOP	ACCELOPS			Jul 9, 2021 1:00:25 AM	Jul 9, 2021 1:50:45 AM
192.168.26.102	00:23:5a:3e:62:69	ANONYMOUS (Domain)	lab02-ws075Cw8-LAPTOP	NT			Jul 9, 2021 1:04:07 AM	Jul 9, 2021 1:54:42 AM
192.168.26.109	00:24:d6:4c:f0:d0	greg.allan (Domain)	greg.allan-LAPTOP	ACCELOPS			Jul 9, 2021 1:00:53 AM	Jul 9, 2021 1:55:20 AM
192.168.64.195	00:0c:29:1e:a1:d8		sdavis-desktop		3	SJ-Main-Cat6500 192.168.20.1 (GigabitEthernet0/11)	Jul 9, 2021 2:00:01 AM	Jul 9, 2021 2:00:01 AM

應用範例三：設備識別與資料統整

詳細檢視設備資訊、資安態勢、效能狀況、組態備份與異動比對

Collect

The screenshot displays the FortiSIEM Configuration Diff interface. A central window titled "Configuration Diff" compares configurations for two devices. The left column shows the current configuration, and the right column shows the previous configuration. A red box highlights the following change:

Device ID	Current Configuration	Previous Configuration
60591	set vlan "Josh"	set vlan "vsw.FortiLink"
60592	set allowed-vlans-all disable	set allowed-vlans-all enable
60593	set allowed-vlans "qtn.FortiLink"	set allowed-vlans-all enable
60594	set untagged-vlans "qtn.FortiLink"	set untagged-vlans "qtn.FortiLink"
60595	set type physical	set type physical
60596	set dhcp-snooping untrusted	set dhcp-snooping untrusted
60597	set dhcp-snoop-option82-trust disable	set dhcp-snoop-option82-trust disable
60598	set arp-inspection-trust untrusted	set arp-inspection-trust untrusted
60599	set igmp-snooping enable	set igmp-snooping enable
60600	set igmps-flood-reports disable	set igmps-flood-reports disable
60601	set igmps-flood-traffic disable	set igmps-flood-traffic disable
60602	set stp-state enabled	set stp-state enabled
60603	set stp-root-guard disabled	set stp-root-guard disabled
60604	set stp-bpdu-guard disabled	set stp-bpdu-guard disabled
60605	set edge-port enable	set edge-port enable
60606	set discard-mode none	set discard-mode none
60607	set packet-sampler disabled	set packet-sampler disabled
60608	set flow-counter-interval 0	set flow-counter-interval 0

Below the diff window, a table lists configuration revisions:

Rev	Date	Type/File Name
109	Aug 17 2021, 09:44:22 AM	startup-config
108	Aug 16 2021, 05:18:41 PM	startup-config
107	Aug 15 2021, 10:09:58 PM	startup-config
106	Aug 15 2021, 01:23:26 PM	startup-config

Navigation buttons: Top, Bottom, Previous, Next, Close.

應用範例四：設備識別與資料統整

CMDB 設備資產盤點 (網路設備含序號資訊)

Collect

The screenshot displays the FortiSIEM interface with the CMDB (Configuration Management Database) report results. The left sidebar shows a navigation menu with 'CMDB Reports' highlighted in red. The main content area shows a table of network device components with the following columns: Device Name, Device Type Vendor, Device Type Model, Component Model, Component Serial, Device Version, and Component Description. The table lists various devices including Cisco, Fortinet, and Avaya models.

Device Name	Device Type Vendor	Device Type Model	Component Model	Component Serial	Device Version	Component Description
3550-Desktop	Cisco	IOS	WS-C3550-24-SMI	CHK0626W1RU	12.2(35)SE	Cisco Catalyst 3550 24 10/100 baseT ports + 2 Gig uplinks fixed configuration Layer 2/3 Ethernet Switch
CoreFW	Fortinet	FortiOS	FGT_501E	FG5H1E5818902695	FortiGate-501E v7.0.0,build0066,210330 (GA)	Fortinet FGT_501E, HW Serial#: FG5H1E5818902695
ERS3510GT	Avaya	ERS	3510GT	12JP240F106W	v5.3.3.015	Ethernet Routing Switch 3510GT
FG240D3913800441	Fortinet	FortiOS	FGT_240D	FG240D3913800441	FortiGate-240D v5.4.1,build1064b1064,160608 (GA)	Fortinet FGT_240D, HW Serial#: FG240D3913800441
FG649	Fortinet	FortiOS	FGT_VM64KVM	FGVM02TM22016519	FortiGate-VM64-KVM v6.4.9,build1966,220421 (GA)	Fortinet FGT_VM64KVM, HW Serial#: FGVM02TM22016519
FGVM04TM22004180	Fortinet	FortiOS	FGT_VM64	FGVM04TM22004180	FortiGate-VM64 v6.4.9,build1966,220421 (GA)	Fortinet FGT_VM64, HW Serial#: FGVM04TM22004180
FortiGate-100F	Fortinet	FortiOS	FGT_100F	FG100FTK19025566	FortiGate-100F v7.0.5,build0304,220208 (GA)	Fortinet FGT_100F, HW Serial#: FG100FTK19025566
FortiGate50B	Fortinet	FortiOS	FGT_50B	FGT50B3G10615108	Fortigate-50B	Fortinet FGT_50B, HW Serial#:



應用範例四：設備識別與資料統整

CMDB 設備資產盤點 (伺服器含安裝軟體資訊)

Collect

The screenshot displays the FortiSIEM interface with the CMDB (Configuration Management Database) report results. The left sidebar shows a navigation menu with 'CMDB Reports' highlighted in red. The main content area shows a table of installed software on Windows servers.

CMDB 報告結果

Windows Installed Software ✕

回上頁 匯出

Device Name	Device IP	Device Type Model	Installed Software Name	Installed Software Vendor	Installed Software Version	Installed Software
W2K12R2SVRTW	10.1.200.182	Windows Server 2012 R2	Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.4974	Microsoft	9.0.30729.4974	Nov 18 2019, 04
W2K12R2SVRTW	10.1.200.182	Windows Server 2012 R2	Microsoft Visual C++ 2010 x64 Redistributable - 10.0.40219	Microsoft	10.0.40219	Nov 18 2019, 04
W2K12R2SVRTW	10.1.200.182	Windows Server 2012 R2	Microsoft Visual C++ 2010 x86 Redistributable - 10.0.40219	Microsoft	10.0.40219	Nov 18 2019, 04
W2K12R2SVRTW	10.1.200.182	Windows Server 2012 R2	Microsoft Visual C++ 2010 x86 Runtime - 10.0.40219	Microsoft	10.0.40219	Nov 18 2019, 04
W2K12R2SVRTW	10.1.200.182	Windows Server 2012 R2	Microsoft Visual Studio 2010 Shell (Isolated) - CHT			Nov 18 2019, 04
W2K12R2SVRTW	10.1.200.182	Windows Server 2012 R2	Microsoft VSS Writer for SQL Server 2012			Nov 18 2019, 04
W2K12R2SVRTW	10.1.200.182	Windows Server 2012 R2	NXLog-CE			Aug 31 2022, 11
W2K12R2SVRTW	10.1.200.182	Windows Server 2012 R2	SQL Server 2012 Common Files			Nov 18 2019, 04
W2K12R2SVRTW	10.1.200.182	Windows Server 2012 R2	SQL Server 2012 Database Engine Services			Nov 18 2019, 04
W2K12R2SVRTW	10.1.200.182	Windows Server 2012 R2	SQL Server 2012 Database Engine Shared			Nov 18 2019, 04
W2K12R2SVRTW	10.1.200.182	Windows Server 2012 R2	SQL Server 2012 Management Studio			Nov 18 2019, 04
W2K12R2SVRTW	10.1.200.182	Windows Server 2012 R2	Sql Server Customer Experience Improvement Program			Nov 18 2019, 04

Copyright © 2022 Fortinet, Inc. All rights reserved. Organization: Super User: admin Scope: Global FortiSIEM 6.6.2.1637



應用範例五：設備識別與資料統整

使用內建日誌解譯器編輯器 (Parser Editor) 調整正規化內容

Collect

The screenshot displays the FortiSIEM interface with the 'Edit Event Parser Definition' window open. The window title is 'Edit Event Parser Definition'. The 'Name' field contains 'FortiGateParser-oldStatus-delta-i' and the 'Device Type' dropdown is set to 'Fortinet FortiOS'. Below these fields are several action buttons: 'Validate', 'Test', 'Reformat', 'Enable', and 'Clear XML'. A search bar with the placeholder '搜尋中...' and 'Previous', 'Next' buttons are also present.

The main area of the window shows XML code for parsing syslog messages. The code includes several `<collectFieldsByRegex>` and `<collectFieldsByKeyValuePair>` tags, along with `<attrKeyMap>` tags for mapping specific fields to attributes. The XML is as follows:

```
10 <case>
11 <collectFieldsByRegex src="$_rawmsg">
12 <regex><![CDATA[<:gPatSyslogPRI><_mon:gPatMon>\s+<_day:gPatDay>\s+<_time:gPatTime>\s+<_body:gPatMesgBody]]></rege
13 x>
14 </collectFieldsByRegex>
15 </case>
16 <case>
17 <collectFieldsByRegex src="$_rawmsg">
18 <regex><![CDATA[<:gPatSyslogPRI>?<_body:gPatMesgBody]]></regex>
19 </collectFieldsByRegex>
20 </case>
21 </switch>
22 <setEventAttribute attr="eventType">"FortiGate-Generic"</setEventAttribute>
23 <setEventAttribute attr="totFlows">1</setEventAttribute>
24 <collectFieldsByKeyValuePair kvsep=" " sep=" " src="$_body">
25 <attrKeyMap attr="sessionId" key="session_id"/>
26 <attrKeyMap attr="sessionId" key="sessionId"/>
27 <attrKeyMap attr="sessionId" key="sessionId"/>
28 <attrKeyMap attr="httpUserAgent" key="agent"/>
29 <attrKeyMap attr="encryptAlgo" key="encryption"/>
30 <attrKeyMap attr="wlanRadioid" key="radioid"/>
31 <attrKeyMap attr="profileDetails" key="applist"/>
32 <attrKeyMap attr="profileDetails" key="policytype"/>
33 <attrKeyMap attr="profileDetails" key="profile"/>
34 </collectFieldsByKeyValuePair>
```

At the bottom of the window, there are '儲存' (Save) and '取消' (Cancel) buttons. The FortiSIEM logo and version number '6.7.2.1727' are visible in the bottom right corner of the interface.



威脅偵測

Detect



應用範例一：威脅與異常行為偵測

內建 AI / ML 關聯規則，協助建立營運基準線並偵測異常行為

Detect

The screenshot shows the FortiSIEM interface with the 'Resources > Rules' page. A search bar at the top contains the word 'sudden'. A list of rules is displayed, with several rows highlighted by red dashed lines. Three callout boxes provide additional context for these rules:

- 基於機器學習 (ML) 基準線與異常行為智能分析**: Points to the first rule, '(s) Sudden Increase in Successful Logons To A Host'.
- 基於經緯度與智能分析**: Points to the sixth rule, '(s) Sudden Increase in WMI Response Times'.
- 基於使用者行為智能分析**: Points to the seventh rule, '(s) Sudden User Location Change'.

已啟用	Severity	Name	Description	Tactic	Impact	System
<input checked="" type="checkbox"/>	7 - MEDIUM	(s) Sudden Increase in Successful Logons To A Host	Detects a sudden 50% increase of successful logons to a host over a 30 minute window	Initial Access, Persistence, Privilege Escalation, Defense Evasion	Valid Accounts: Local Accounts (T1078.003)	System
<input checked="" type="checkbox"/>	7 - MEDIUM	(s) Sudden Increase In System CPU Usage	Detects sudden increase in CPU usage - current average over 30 minute interval is more than 3 standard deviations away from the mean and the current average is at least 50 percent	Impact	Endpoint Denial of Service: OS Exhaustion Flood (T1499.001)	System
<input checked="" type="checkbox"/>	7 - MEDIUM	(s) Sudden Increase in System Memory Usage	Detects a sudden increase in system memory usage - over a 30 minute interval, either the physical or virtual memory is 25% more than the statistical average over that same time period and the current physical memory usage is at least 50%	Impact	Endpoint Denial of Service: OS Exhaustion Flood (T1499.001)	System
<input checked="" type="checkbox"/>	7 - MEDIUM	(s) Sudden Increase in User Login Volume	Detects daily user login volume anomaly against profile. This may indicate suspicious user behaviors.			System
<input checked="" type="checkbox"/>	7 - MEDIUM	(s) Sudden Increase in WMI Response Times	Detects a sudden 50% increase of WMI Response Times over a 30 minute time window	Imp		
<input checked="" type="checkbox"/>	9 - HIGH	(s) Sudden User Location Change	Detects location change for a user unfeasible in the period of time. This may indicate a stolen credential.			
<input checked="" type="checkbox"/>	7 - MEDIUM	(s) Sudden User Login Pattern Change	Detects daily user login distribution anomaly against profile. This may indicate suspicious user behaviors.			System



應用範例二：威脅與異常行為偵測

整合情資黑名單 (FortiGuard Lab) · 快速發現可疑的對外連線

Detect

The screenshot displays the FortiSIEM interface. The top navigation bar includes '儀表板', '關聯分析', '告警事故', '派工管理', 'CMDB', '資源庫', '工作', and '系統管理'. The main content area is titled '資源庫 > Malware IPs > FortiGuard Malware IP'. A sidebar on the left lists various malware categories, with 'FortiGuard Malware IP' highlighted in a red box. The main table shows a list of active malware IPs with columns for 'Active', 'Low IP', 'Malware Type', 'Country', 'Description', 'Date Found', and 'Last Seen'. The table contains 12 rows of data, all with a 'Date Found' of '00:11:56' and 'Last Seen' of '12/13/2022 CST'. The 'Description' for all entries is 'Spyware and Malware'.

Active	Low IP	Malware Type	Country	Description	Date Found	Last Seen
<input checked="" type="checkbox"/>	100.0.0.0	Malware/CnC		Spyware and Malware	00:11:56	12/13/2022 CST
<input checked="" type="checkbox"/>	100.0.41.228	Malware/InstallationTraffic		Spyware and Malware	00:11:56	12/13/2022 CST
<input checked="" type="checkbox"/>	100.1.106.211	Malware/InstallationTraffic		Spyware and Malware	00:11:56	12/13/2022 CST
<input checked="" type="checkbox"/>	100.1.108.111	Malware/CnC		Spyware and Malware	00:11:56	12/13/2022 CST
<input checked="" type="checkbox"/>	100.1.108.129	Malware/CnC		Spyware and Malware	00:11:56	12/13/2022 CST
<input checked="" type="checkbox"/>	100.1.108.131	Malware/CnC		Spyware and Malware	00:11:56	12/13/2022 CST
<input checked="" type="checkbox"/>	100.1.108.142	Malware/CnC		Spyware and Malware	00:11:56	12/13/2022 CST
<input checked="" type="checkbox"/>	100.1.108.16	Malware/CnC		Spyware and Malware	00:11:56	12/13/2022 CST
<input checked="" type="checkbox"/>	100.1.108.193	Malware/CnC		Spyware and Malware	00:11:56	12/13/2022 CST
<input checked="" type="checkbox"/>	100.1.108.203	Malware/CnC		Spyware and Malware	00:11:56	12/13/2022 CST



應用範例二：威脅與異常行為偵測

整合情資黑名單 (第三方或自行定義情資)，快速發現可疑的對外連線

Detect

The screenshot shows the FortiSIEM interface for configuring Malware IPs. The main menu includes: 儀表板, 關聯分析, 告警事故, 派工管理, CMDB, 資源庫, 工作, 系統管理. The breadcrumb path is 資源庫 > Malware IPs > BlackList. The left sidebar lists various Malware IP sources, with BlackList selected. The main content area has buttons for 新增, 編輯, 刪除, 更多, and a search bar. A modal window titled "更新 惡意軟體 IP 地址" is open, showing two radio button options: "從 CSV 檔案匯入" (selected) and "更新透過 API". The "更新透過 API" option is expanded, showing a "URL:" field with the value "http://abc.corp.com/internal_ip_blacklist.txt" and a "排程:" field with the value "Scheduled for: every 1 day at 00:00 AM starting 12/15/2022.". Both the URL and the schedule fields are highlighted with red boxes. The modal also includes edit and delete icons for the URL and a "關閉" button at the bottom.



應用範例三：威脅與異常行為偵測

Detect

利用突發威脅告警相關之關聯規則、報表樣板，偵測、回溯及威脅獵捕可能的潛伏威脅

The screenshot displays the FortiSIEM interface for Threat Hunting. The left sidebar shows a navigation menu with 'Reports' highlighted in red. The main content area shows a table of reports with columns for Name, Description, Scope, and Report Design Template. The table lists various reports such as 'Linux file timestomping via touch', 'Linux internal reconn', and 'Log4J Exploit Request Detected By Regex'.

Name	Description	Scope	Report Design Template
Linux file timestomping via touch	Reports file timestamp modification by using touch command. Requires FSM Linux Agent or Crowdstrike Data Replicator logs.	System	Global System Reports Roc
Linux internal reconn	Reports Linux internal reconnaissance attempts via commands such as ifconfig, whoami etc. Requires FSM Linux Agent or Crowdstrike Data Replicator logs.	System	Global System Reports Roc
Linux Successful and Failed sudo	Reports Successful and Failed sudo executions on Linux systems. Requires Linux SSH access logs.	System	Global System Reports Roc
Log4J Exploit Request Detected By Regex	Log4J Exploit Request Detected by Regex. Regex Inspection of http user agent, referrer, cookie, content type, and cache control for Log4J CVE-2021-44228.	System	Global System Reports Roc
Log4J Exploit Request Detected on Host by Fortinet Products	Log4J Exploit Request Detected on Host by Fortinet Product. IPS signature ID 51006 for Log4J CVE-2021-44228 seen by a Fortinet product.	System	Global System Reports Roc
Log4J Exploit Request Detected on Network by Fortinet Products	Log4J Exploit Request Detected on Network by Fortinet Product. IPS signature ID 51006 for Log4J CVE-2021-44228 seen by a Fortinet product.	System	Global System Reports Roc
Malware activity - A afraidGate	Finds activity Associated with A afraidGate Malware. Requires FSM Windows Agent or Crowdstrike Data Replicator logs.	System	Global System Reports Roc
Malware activity - Angler	Finds activity Associated with Angler Malware. Requires sysmon logs via FSM Windows Agent or Crowdstrike Data Replicator logs.	System	Global System Reports Roc
Malware activity - InPage - Domain match	Find activity Associated with InPage Malware by domain match. Requires DNS logs from FSM Windows Agent or Crowdstrike Data Replicator logs.	System	Global System Reports Roc
Malware activity - Sage 2.0 - Domain match	Find activity Associated with Sage 2.0 Malware by domain match. Requires DNS logs from FSM Windows Agent or Crowdstrike Data Replicator logs.	System	Global System Reports Roc



應用範例四：威脅與異常行為偵測

Detect

MITRE ATT&CK 資安對抗策略、手段告警圖，顯示進階持續性威脅 (Advanced Persistence Threat) 發生的各個階段

The screenshot displays the FortiSIEM interface for MITRE ATT&CK Incident Explorer. The top navigation bar includes options like '儀表板', '關聯分析', '告警事故', '派工管理', 'CMDB', '資源庫', '工作', and '系統管理'. The main content area shows a table with columns for various MITRE ATT&CK tactics and their occurrence counts across different assets.

設備	Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
aw9001			2		13	6	6	2				2	4	
TR1	1		1	2	1			2	1	1		1		
211.141.78.56			1		1					1		1		
150.109.116.15													4	
54.209.131.199				2										
www.abcd.z2.dca1.com												1		
www.xyz.z1.dca0.com												1		
221.229.172.66				1										

Below the table, there is a section for '相關告警事故' (Related Alerts) with columns for severity, time, alert name, tactic, technique, source, target, details, alert status, and resolution status.

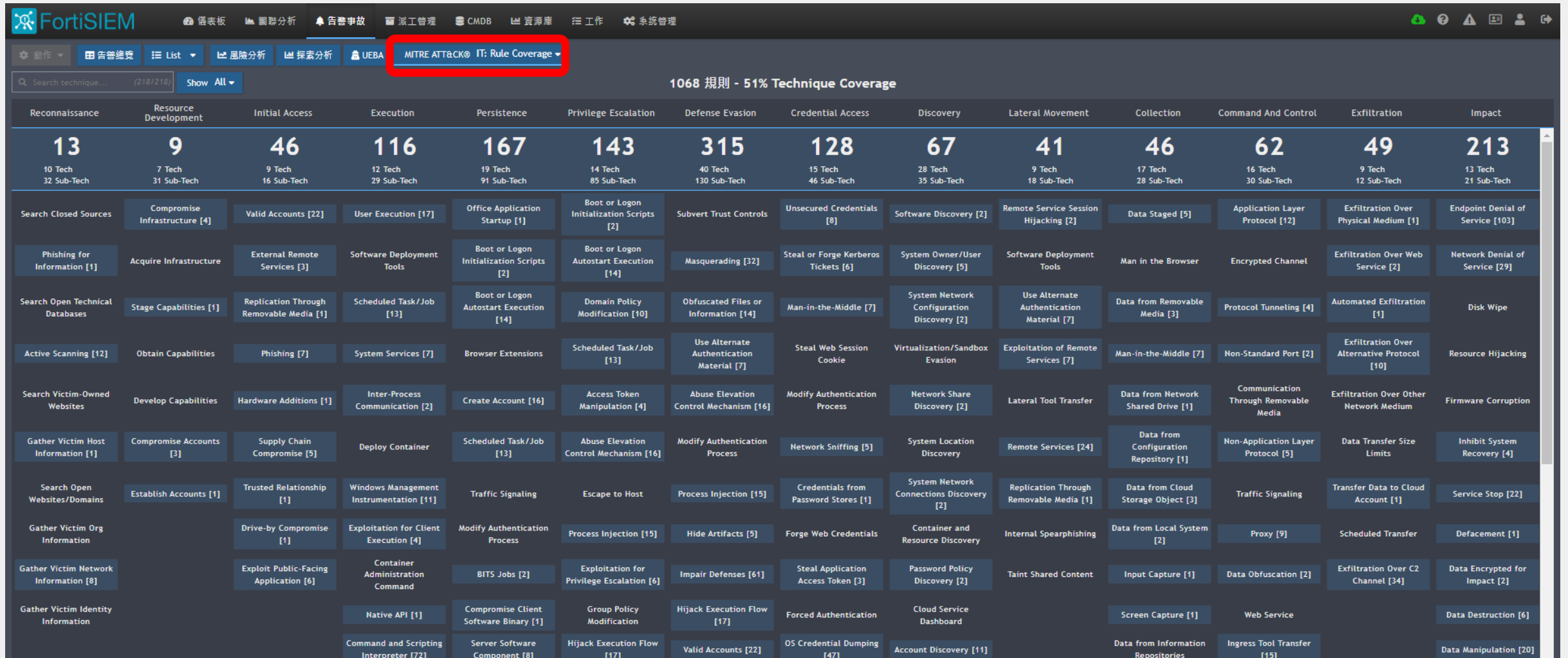
嚴重性類別	最後一次發生	告警事故	戰術	技術	來源	目標	詳細資訊	告警事故狀態	解決處理狀態
MEDIUM	Oct 15 2021, 01:50:30 PM	Windows User Added to Groups	Persistence	Account Manipulation: ...	AW9001	User: administrator Target User: Users	...	Active	Open
MEDIUM	Oct 15 2021, 01:50:30 PM	Windows User Password Changed	Persistence	Account Manipulation: ...	AW9001	User: Administrator Target User: Admini...	...	Active	Open



MITRE ATT&CK 資安對手策略、技術手法

關聯規則對應 MITRE ATT&CK 新資安框架 (Enterprise & ICS)

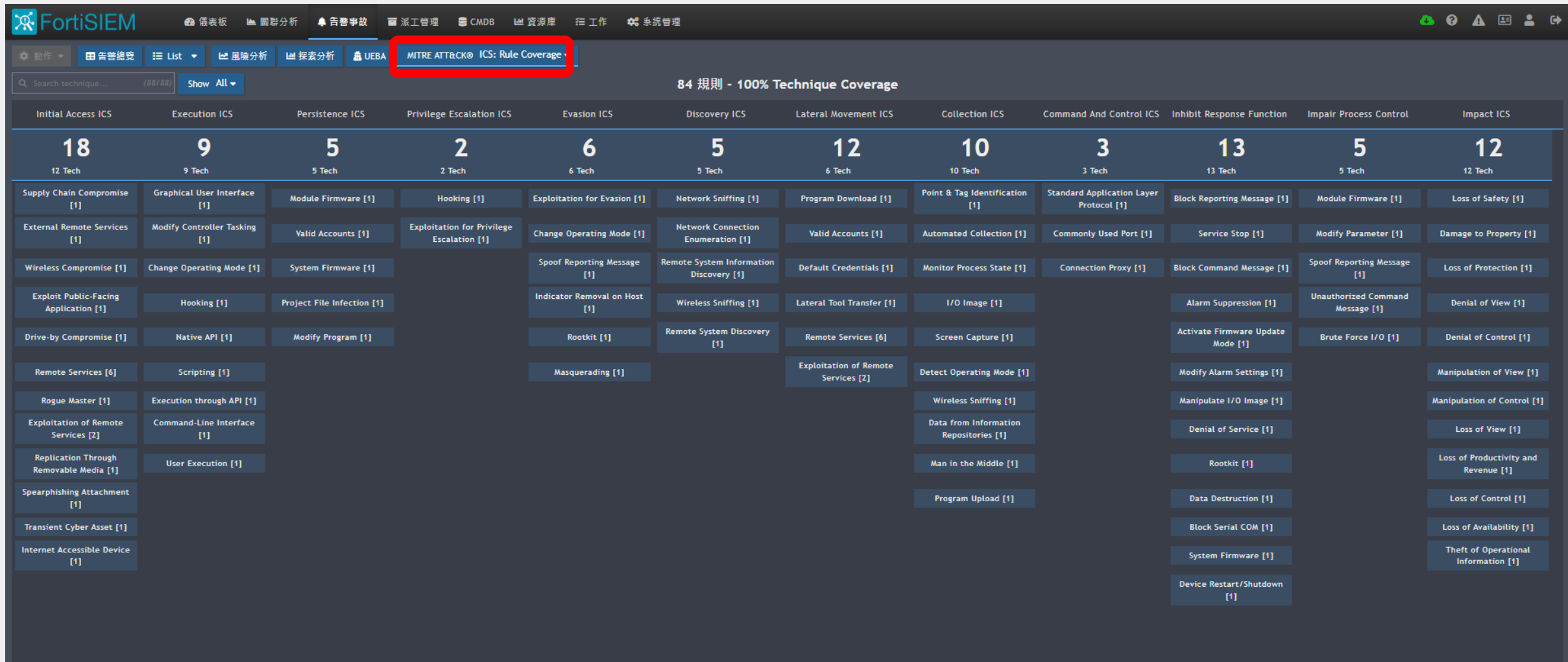
告警圖



MITRE ATT&CK 資安對手策略、技術手法

關聯規則對應 MITRE ATT&CK 新資安框架 (Enterprise & ICS)

告警圖



維運監看

Monitor



應用範例一：維運監看 (告警總覽)

所有告警事故分類、告警事故排行，受影響設備排行

Monitor



應用範例二：維運監看 (設備一覽表)

Monitor

設備資安、效能、可用度一目瞭然

Demo Dashboard | Demo X | 台北 X

搜尋... | All Severities | All Organizations | 全部位置 | Table View | 3 分鐘 | 1/1 | 16

Maint	Device	IP	Type	Organization	Avail Status	Packet Loss	Uptime	Uptime %	Perf Status	Sec Status	CPU Util	Mem Util	Disk Util	Fr
●	W2K8R2SVREN	10.1.200.181	Microsoft Windows Server 2008 R2	SE_Lab	●	0%	115 days	100%	●	●	3%	51%	47%	3
●	w2k12r2svrtw-dc.se_lab.ftnt.com...	10.1.200.185	Microsoft Windows Server 2012 R2	SE_Lab	●	0%	109 days	100%	●	⚠	6%	47%	28%	4
●	FMG-VM64_v7	10.1.200.2	Fortinet FortiManager	SE_Lab	●	0%	69 days	100%	●	●	1%	23%	23%	7
●	VW64GB	10.1.200.200	VMware ESXi Server	SE_Lab	●	0%	115 days	100%	✖	●	11%	93%	95%	30
●	LAB-1500D	10.1.200.254	Fortinet FortiOS	SE_Lab	●	0%	5 days	100%	⚠	⚠	3%	33%	0%	10
●	ERS3510GT	10.1.210.35	Avaya ERS	SE_Lab	●	0%	10 days	100%	⚠	●	18%	84%		
●	3550-Desktop	10.1.215.87	Cisco IOS	Super	●	0%	401 days	100%	●	●	5%	30%		
●	Paul-Desktop-2960	10.1.215.97	Cisco IOS	Super	●	0%	10 hours	26%	●	●	7%	26%		
●	LAB_Switch_01	172.16.101.1	Fortinet FortiSwitch	SE_Lab	●	0%	477 days	100%	●	●	53%	50%		
●	Video_Room_01	172.16.101.11	Fortinet FortiSwitch	SE_Lab	●	0%	477 days	100%	⚠	●	24%	70%		
●	Rack_F_to_A	172.16.101.2	Fortinet FortiSwitch	SE_Lab	●	0%	477 days	100%	●	●	19%	48%		
●	Rack_F_to_B	172.16.101.4	Fortinet FortiSwitch	SE_Lab	●	0%	477 days	100%	●	●	10%	17%		
●	LAB_Switch_02	172.16.101.5	Fortinet FortiSwitch	SE_Lab	●	0%	477 days	100%	●	●	44%	49%		
●	LAB_Switch_03	172.16.101.6	Fortinet FortiSwitch	SE_Lab	●	0%	477 days	100%	●	●	48%	49%		
●	Rack_F_to_D	172.16.101.8	Fortinet FortiSwitch	SE_Lab	●	0%	477 days	100%	●	●	34%	24%		
●	Rack_F_to_I	172.16.101.9	Fortinet FortiSwitch	SE_Lab	●	0%	111 days	100%	●	●	45%	46%		

應用範例三：維運監看 (資安設備)

Monitor

我的儀表板 (Global) ▾

防火牆 ✕

網路交換器 ✕

端點偵測與回應 ✕

伺服器 ✕

NetFlow/sFlow ✕

Identity & Location ✕

+ ▾

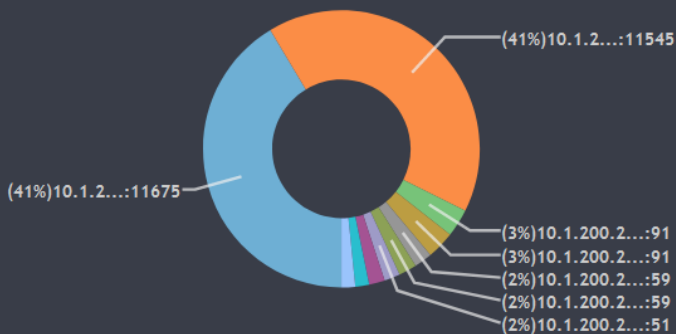
排版: 版塊 ▾

📄 📄 🔄 🗑️

防火牆事件類別分析

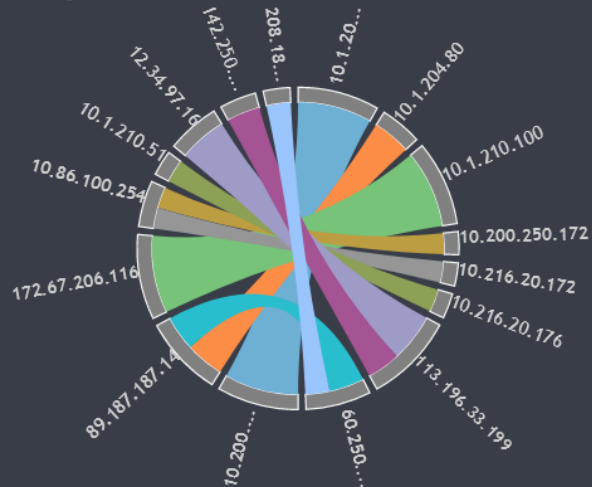
Last 1 hour@14:59

COUNT(Matched Events)



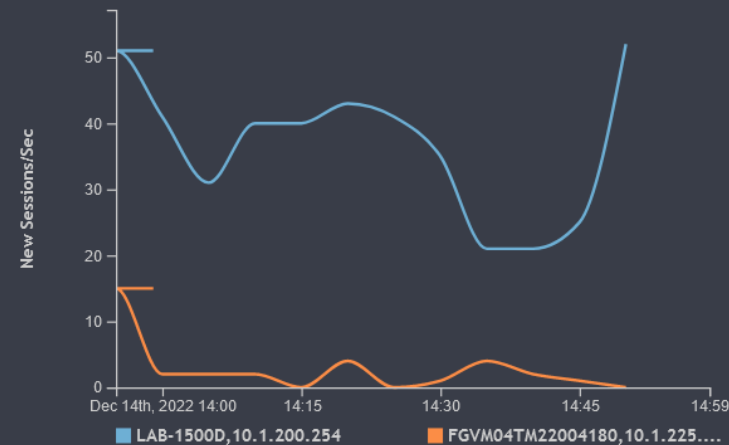
防火牆會談流量分析

Last 1 hour@14:59



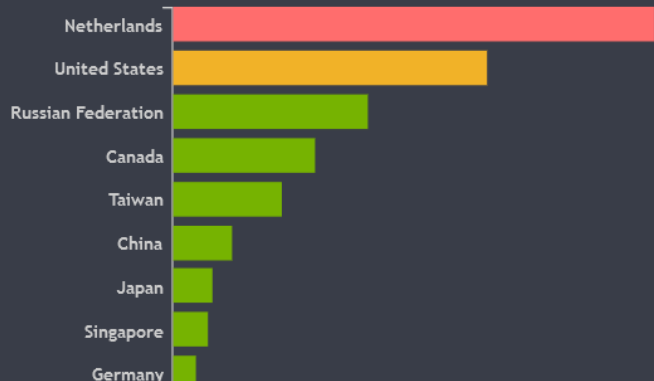
防火牆新建會談速率

Last 1 hour@14:59



防火牆來源國家分析

Last 1 hour@14:59



防火牆目的地國家排行榜

Last 1 hour@14:59



終端設備廠牌與作業系統分析

Last 1 hour@14:59



應用範例四：維運監看 (網路設備)

Monitor

我的儀表板 (Global) ▾

防火牆 ✕

網路交換器 ✕

端點偵測與回應 ✕

伺服器 ✕

NetFlow/sFlow ✕

Identity & Location ✕

+

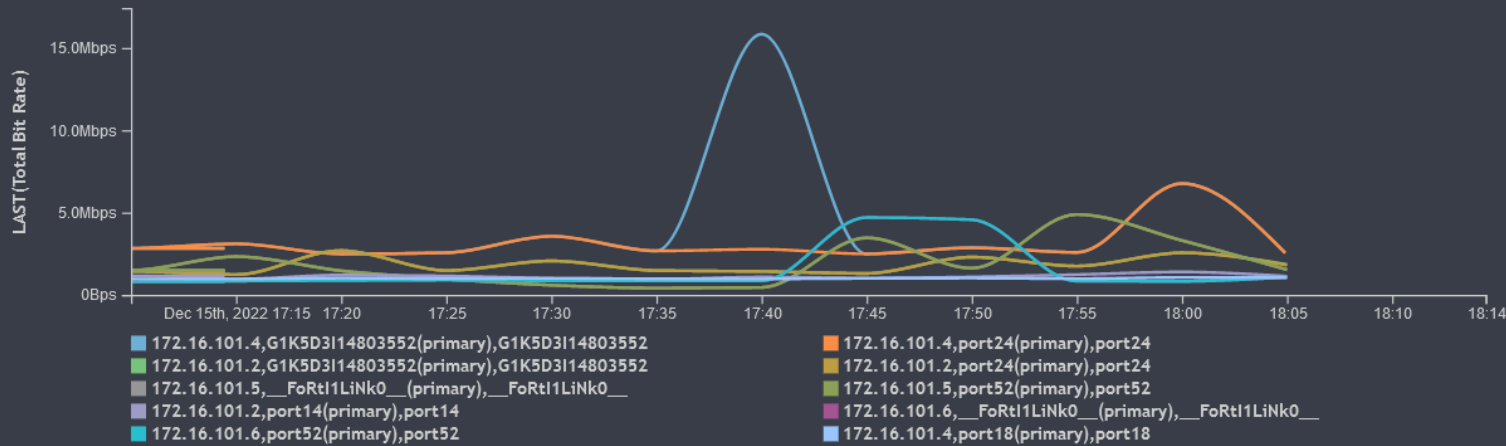
Y

排版: 版塊 ▾

📄 📄 🔄 🗑️

網路交換器介面流量分析

Last 1 hour@18:14



網路交換器系統資源用量分析 (CPU Util)

Last 1 hour@18:14

Reporting IP	LAST(CPU Util)	Trend
172.16.0.4	63%	
172.16.101.6	44%	
172.16.101.5	36%	
172.16.101.9	34%	
192.168.19.1	34%	
172.16.101.1	31%	
172.16.101.11	27%	
172.16.101.2	27%	

網路交換器登入成功/失敗

Last 1 hour@18:15

Event Time	Reporting Device	Reporting IP	User	Source IP	Method	Status
05:59:32 PM	Video_Room_01	172.16.101.11	jim	10.1.210.100	ssh	failed
05:59:31 PM	Video_Room_01	172.16.101.11	jim	10.1.210.100	ssh	failed
05:59:24 PM	Video_Room_01	172.16.101.11	jim	10.1.210.100	ssh	failed
05:58:32 PM	Video_Room_01	172.16.101.11	admin	10.1.210.100	https	success
05:57:57 PM	Video_Room_01	172.16.101.11	admin	10.1.210.100	ssh	success
05:54:37 PM	Video_Room_01	172.16.101.11	fsm	10.1.210.100	https	success

網路交換器系統資源用量分析 MAX(Memory Util)

Last 1 hour@18:14

Reporting IP	MAX(Memory Util)	Trend
10.1.210.35	83.59%	
172.16.101.11	70.74%	
172.16.0.4	51%	
172.16.101.1	50.11%	
172.16.101.6	48.95%	
172.16.101.5	48.85%	

應用範例五：維運監看 (端點安全)

Monitor

我的儀表板 (Global) | 防火牆 | 網路交換器 | 端點偵測與回應 | 伺服器 | NetFlow/sFlow | Identity & Location

+ | 圖表

排版: 區塊 | 上傳 | 下載 | 刷新 | 刪除

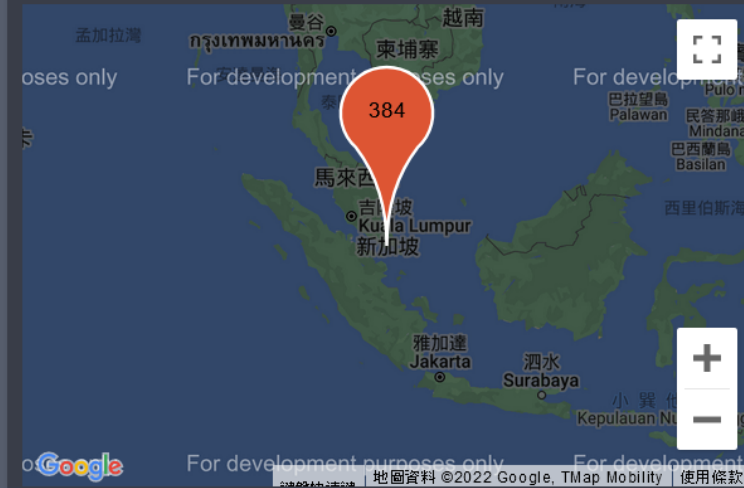
安全事件統計 (依規則)

Last 8 hours@15:09

Event Name	Firewall Action	Rule Name	COUNT(Matched Events)
FortiEDR blocked inconclusive file	Blocked (Simulation)	Dynamic Code - Malicious Runtime...	9216
FortiEDR blocked suspicious file	Blocked (Simulation)	Dynamic Code - Malicious Runtime...	5056
FortiEDR-Security-PUP-Logged	Logged	Unconfirmed File Detected	1152
FortiEDR blocked malicious file	Blocked (Simulation)	Malicious File Detected	1088
FortiEDR blocked suspicious file	Blocked	Dynamic Code - Malicious Runtime...	384
FortiEDR-Security-FortiEDR-Syslog-message-FortiEDR-Sy...	FortiEDR Syslog message		256
FortiEDR blocked malicious file	Blocked (Simulation)	Unconfirmed Executable - Execut...	192
FortiEDR-Security-PUP-Blocked	Blocked (Simulation)	Malicious File Detected	192
FortiEDR blocked suspicious file	Blocked	Suspicious Application - Connecti...	128

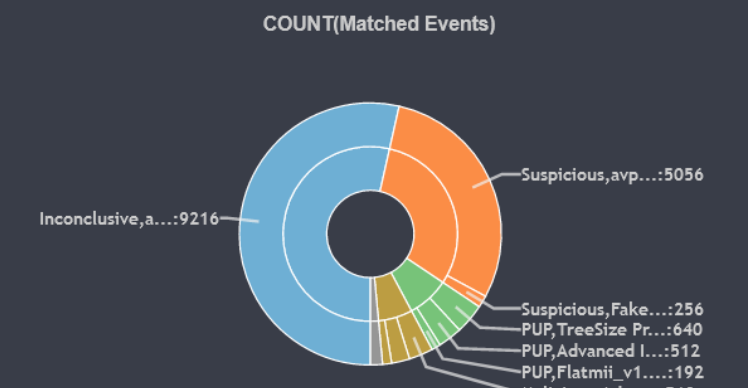
資安事件外部IP統計

Last 8 hours@15:09



可疑應用程式統計

Last 8 hours@15:09



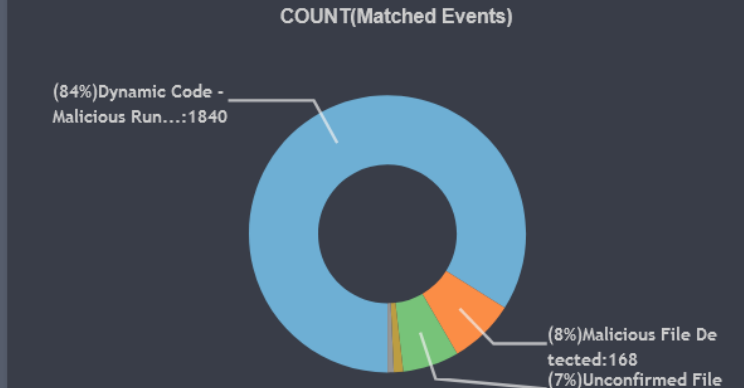
惡意檔案統計 (依來源)

Last 8 hours@15:09

Source IP	File Name	COUNT(Matched Events)
192.168.1.155	avp.exe	14k
10.1.1.8	Advanced IP Address ...	512
10.1.1.8	Advanced Port Scann...	512
10.1.1.8	TreeSize Professional...	512
10.1.1.8	keygen.exe	384
192.168.1.69	Fake Minecraft Instal...	256
192.168.1.155	Flatmii_v1.5.exe	192

規則使用排行榜

Last 1 hour@15:09



應用範例六：維運監看 (主機設備)

Monitor

我的儀表板 (Global) -

防火牆 ✕

網路交換器 ✕

端點偵測與回應 ✕

伺服器 ✕

NetFlow/sFlow ✕

Identity & Location ✕

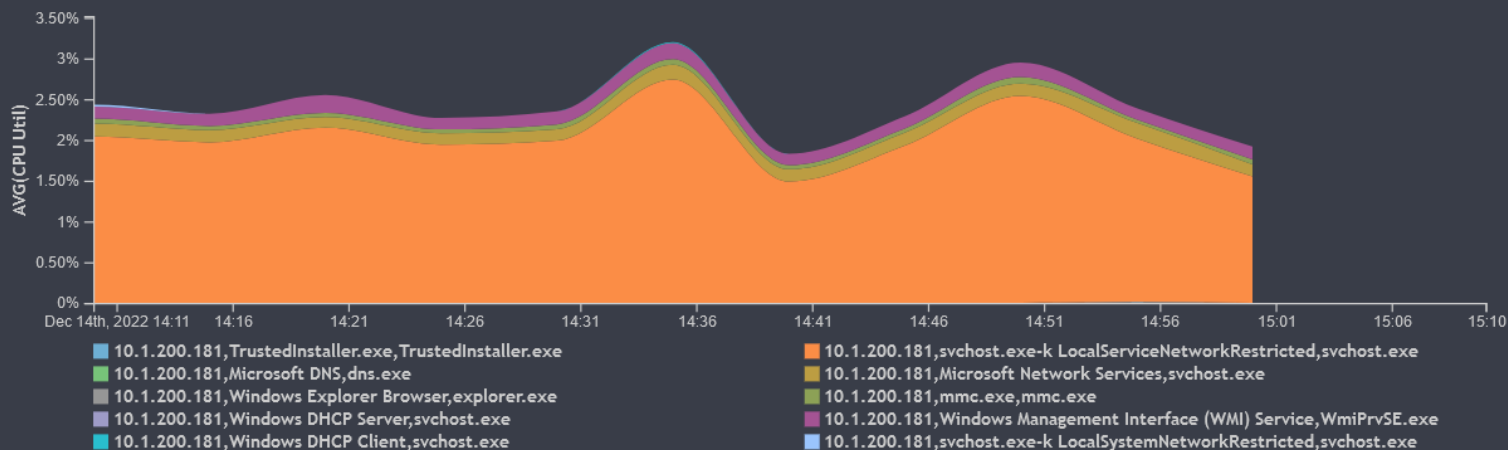
+ T

排版: 版塊 -

📄 ⬇️ ⬆️ 🔄 🗑️

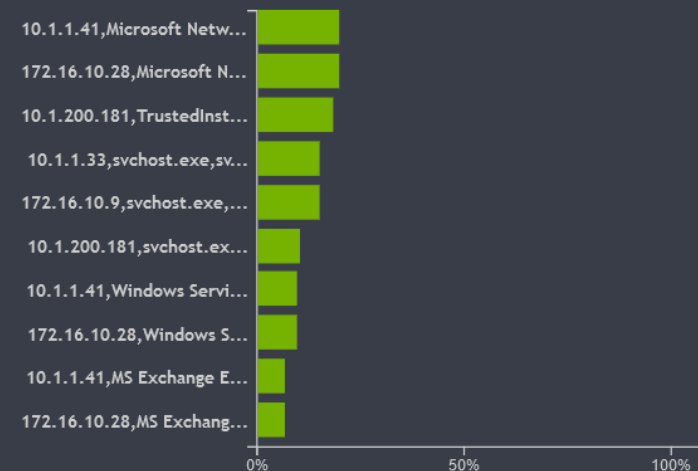
Windows 程式CPU資源使用率分析 (平均值)

Last 1 hour@15:10



Windows 程式記憶體資源使用率分析 (最大值)

Last 1 hour@15:10



Windows 登入失敗記錄

Last 1 hour@15:10

Event Receive Time	User	Server
Dec 14 2022, 02:34:27 PM	matt	W2K8R2SVRTW
Dec 14 2022, 02:34:27 PM	kevin	W2K8R2SVREN
Dec 14 2022, 02:34:27 PM	jim	W2K8R2SVRTW
Dec 14 2022, 02:34:26 PM	kevin	W2K8R2SVREN
Dec 14 2022, 02:34:26 PM	vincent	W2K8R2SVREN
Dec 14 2022, 02:34:26 PM	vincent	W2K8R2SVREN

Windows 檔案異動記錄

Last 1 hour@15:10

Event Receive Time	Server	User	Action	File Name
Dec 14 2022, 02:34:26 PM	W2K8R2SVREN	summer	Modified	c:\zone\新產品發表計畫書.txt
Dec 14 2022, 02:34:26 PM	W2K8R2SVREN	gary	Modified	c:\zone\員工薪資查核表.rtf
Dec 14 2022, 02:34:26 PM	W2K8R2SVREN	lily	Added	c:\zone\New Rich Text Document.rtf
Dec 14 2022, 02:34:26 PM	W2K8R2SVREN	gary	Removed	c:\zone\十月內部稽核會議記錄.txt
Dec 14 2022, 02:34:26 PM	W2K8R2SVREN	gary	Removed	c:\zone\九月內部稽核會議記錄.txt
Dec 14 2022, 02:34:25 PM	W2K8R2SVREN	gary	Modified	c:\zone\公司Q1財報會議記錄.rtf
Dec 14 2022, 02:34:25 PM	W2K8R2SVREN	gary	Modified	c:\zone\員工通訊錄.txt

應用範例七：維運監看 (流量分析)

Monitor

我的儀表板 (Global) ▾

防火牆 ✕

網路交換器 ✕

端點偵測與回應 ✕

伺服器 ✕

NetFlow/sFlow ✕

Identity & Location ✕

+

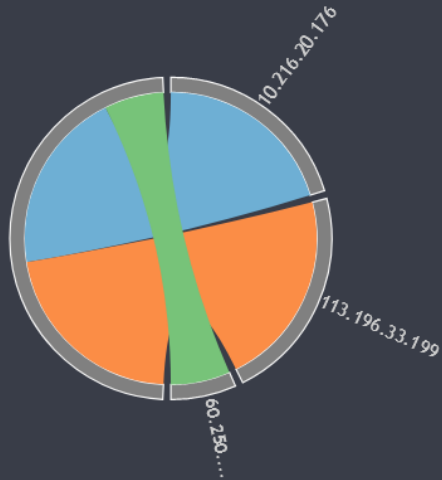
▽

排版: 版塊 ▾



sFlow_nFlow: Top Conversations By Bytes ✕

Last 1 hour@15:11



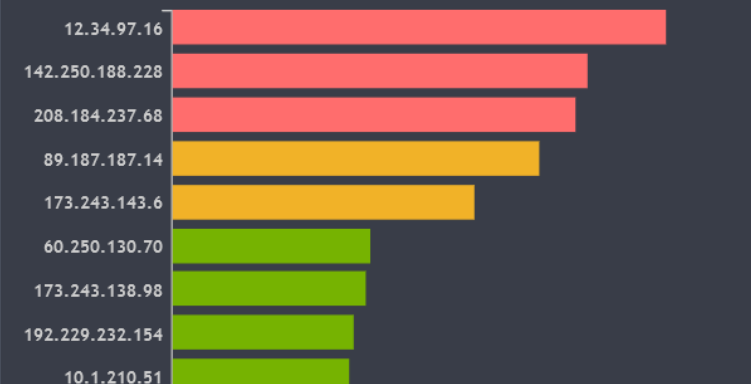
sFlow_nFlow: Top Conversations By Bytes ✕

Last 1 hour@15:11

Source IP	Source Host Name	Destination IP	Flows	Total	Sent	Recv
113.196.33.199		12.34.97.16	9	150.9...	3.27 ...	147.6...
60.250.130.70		89.187.187.14	2	118.5...	2.6 MB	115.9...
113.196.33.199		142.250.188.228	121	115.3...	9.85 ...	105.4...
60.250.130.70		173.243.143.6	12	97.29...	1.6 MB	95.68...
60.250.130.70		208.184.237.68	8	79.53...	750 KB	78.8 ...
113.196.33.199		173.243.138.98	6	62.35...	1.54 ...	60.8 ...
113.196.33.199		192.229.232.154	5	58.49...	1.2 MB	57.29...
10.216.20.176		10.1.210.51	43	57.41...	8.26 ...	49.15...
113.196.33.199		35.235.123.194	46	45.15...	34.6 ...	10.54...

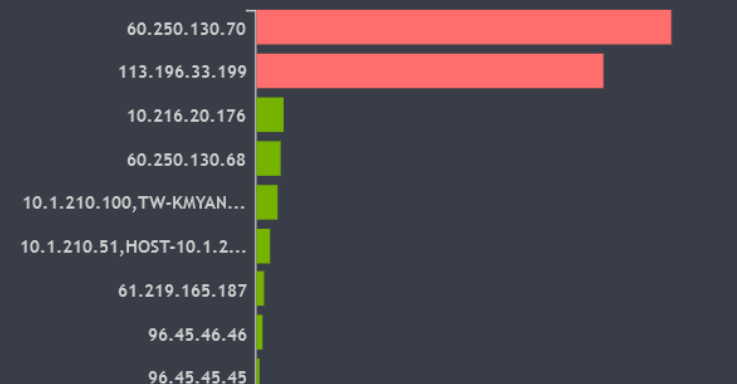
sFlow_nFlow: Top Destination IPs By Bytes ✕

Last 1 hour@15:11



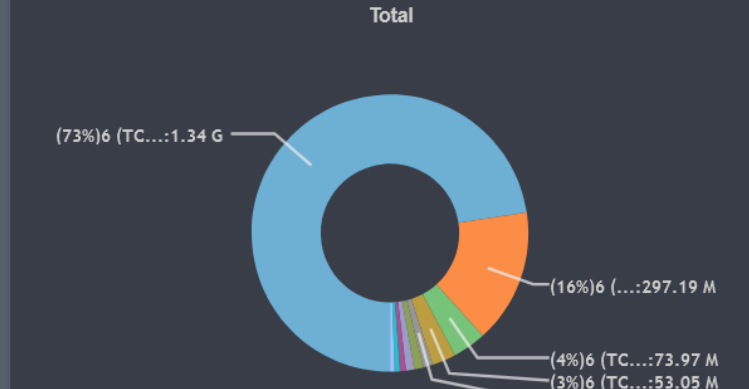
sFlow_nFlow: Top Source IPs By Bytes ✕

Last 1 hour@15:11



sFlow_nFlow: Top Protocols By Byte ✕

Last 1 hour@15:11



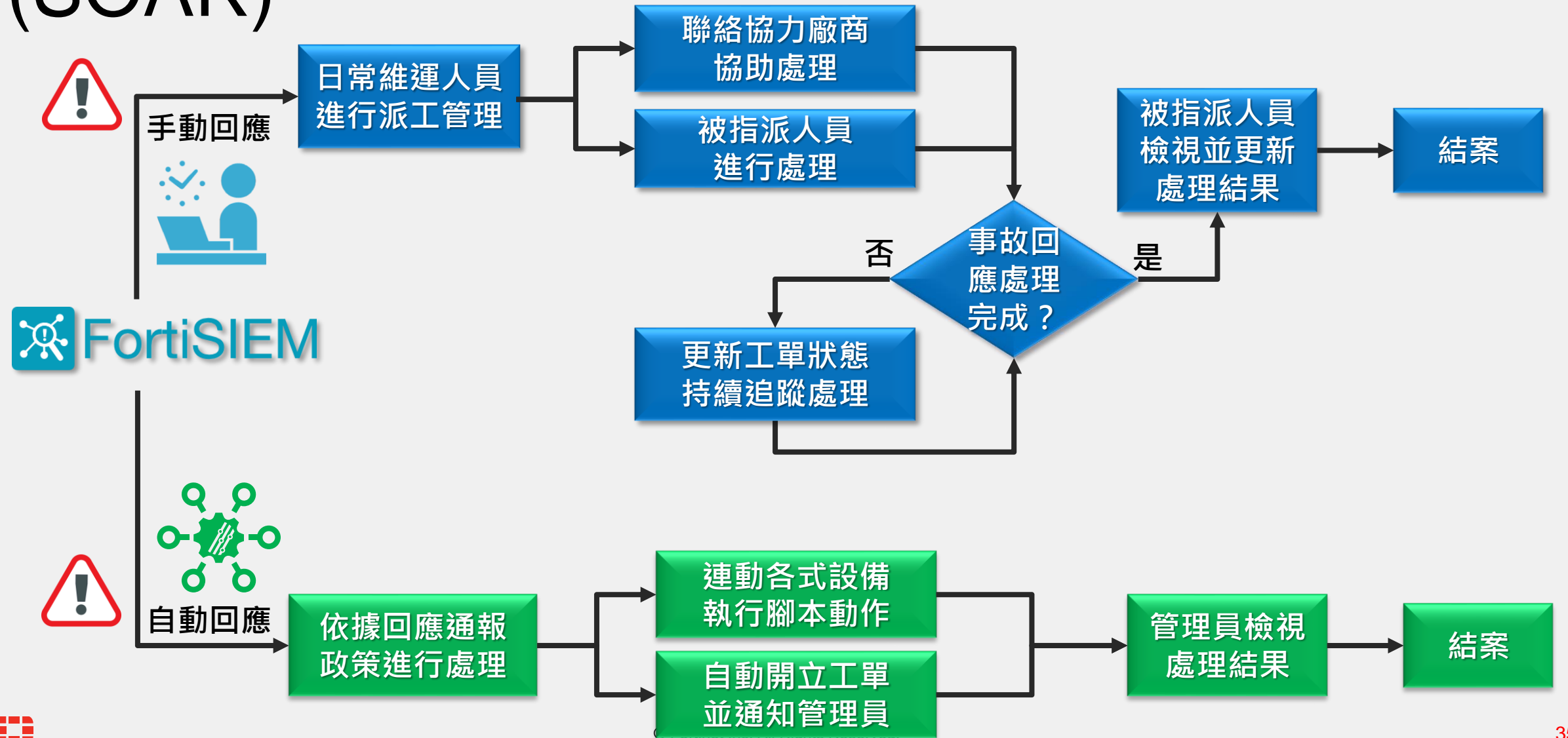
事故回應

Respond



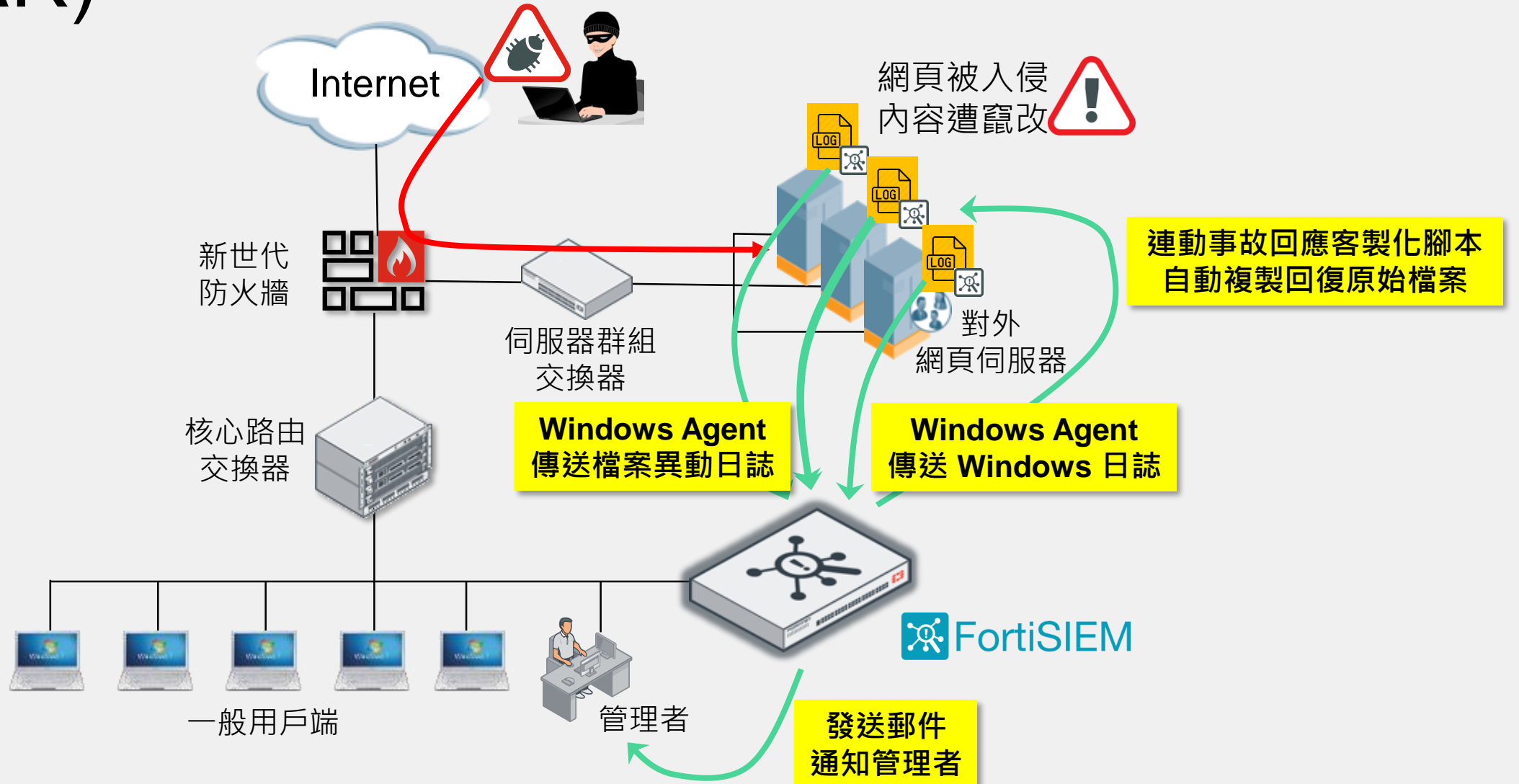
應用範例一：告警事故協作回應與自動 Respond

手動與自動化告警事故回應流程 (SOAR)



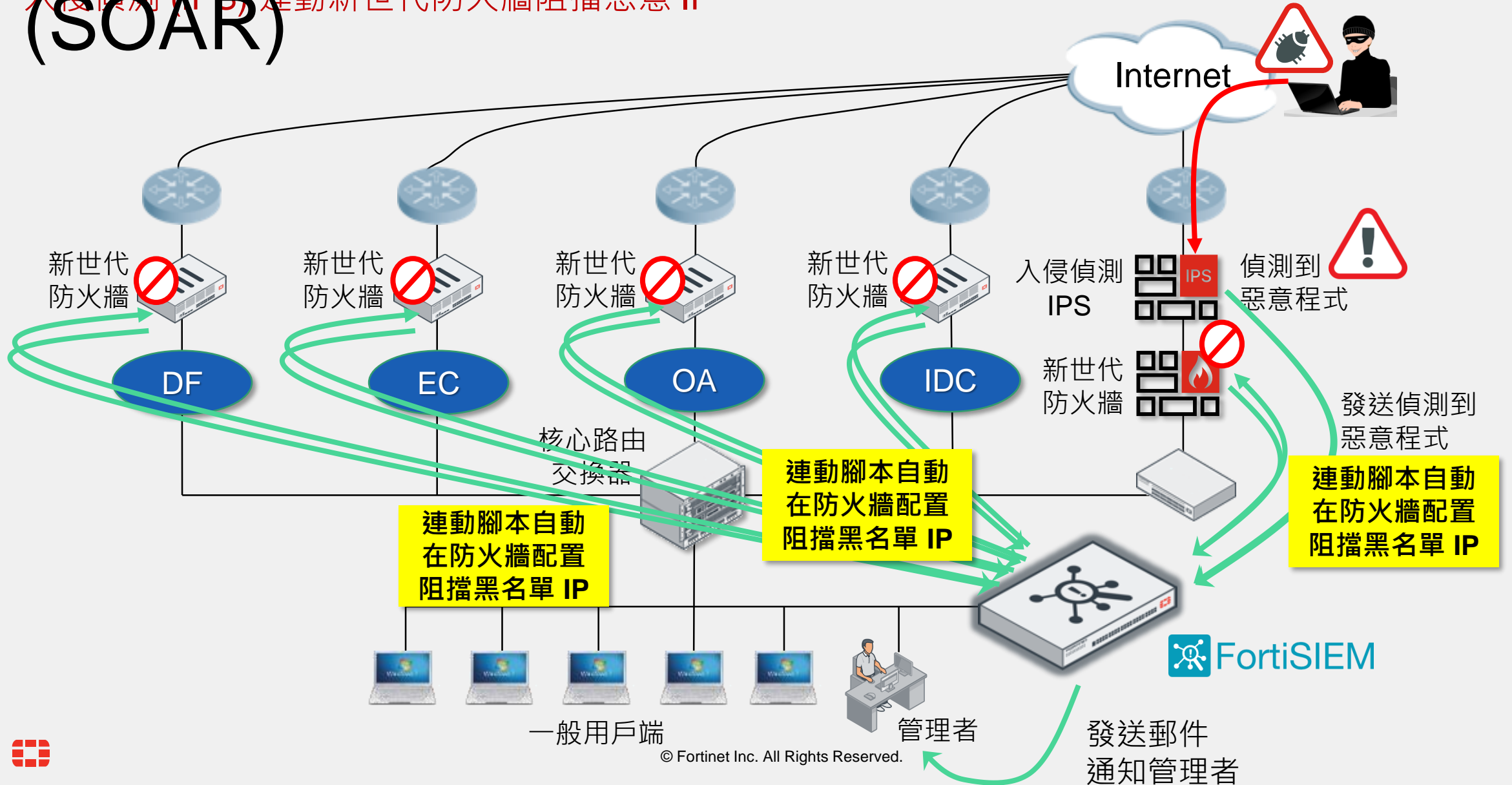
應用範例二：告警事故協作回應與自動 Respond

檔案異動偵測連動網頁竊改復原機制 (SOAR)



應用範例三：告警事故協作回應與自動 Respond

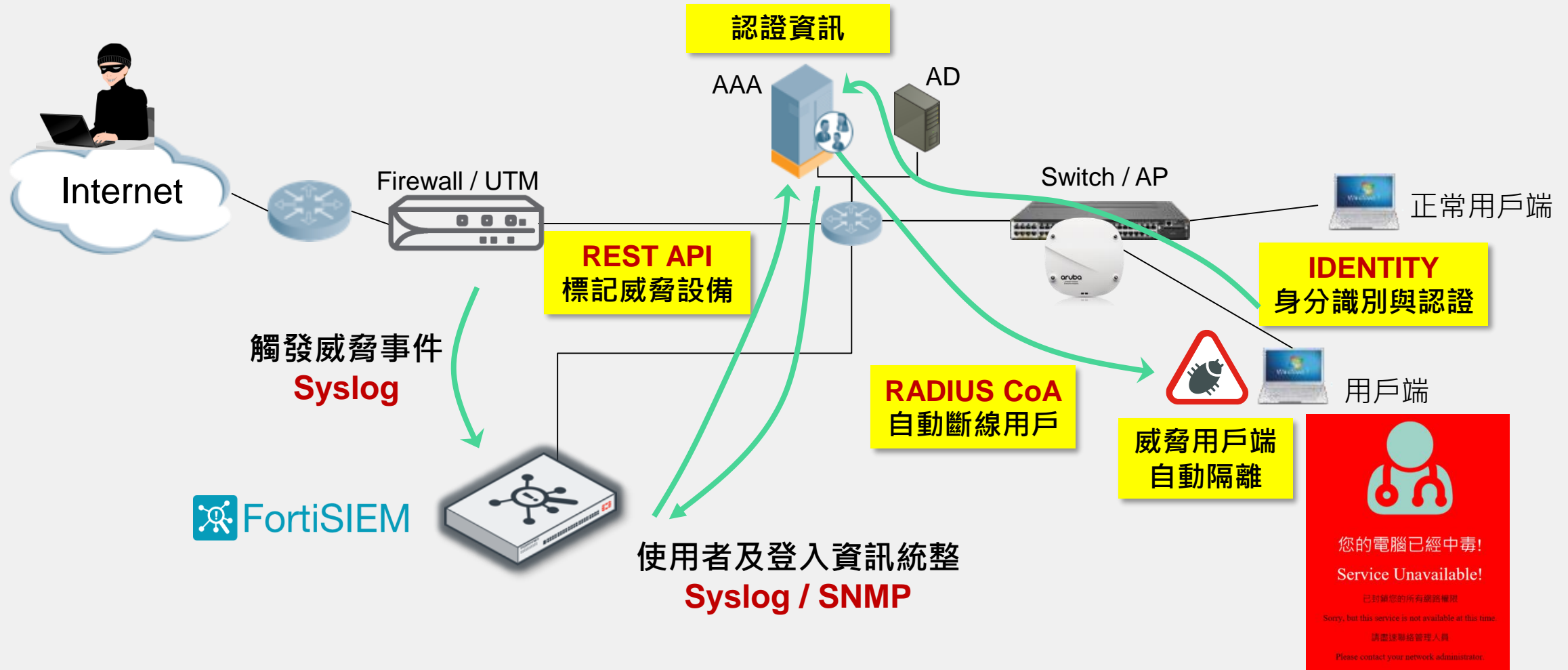
入侵偵測 (IPS) 連動新世代防火牆阻擋惡意 IP (SOAR)



應用範例四：告警事故協作回應與自動 **Respond**

使用者(有線/無線) 入網異常行為監看與自動隔離

(SOAR)



FortiSIEM 重要特點與價值

資料統整、威脅偵測、維運監看、事故回應一氣呵成



各種資訊匯集統整，日誌稽核，合規報表，安全資訊與事件管理 (SIEM)



還可以作為資安/網維管理的優化工具



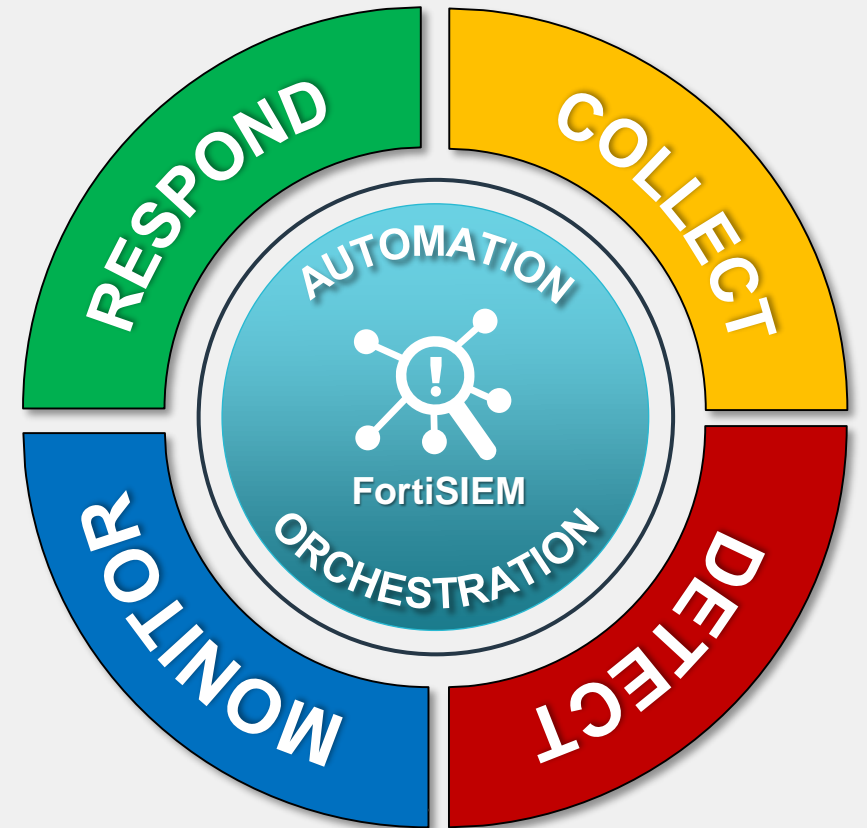
AI / ML 智能關聯分析，對應 MITRE 資安框架，提供威脅先期預警能力



彈性的資安/網維儀表板提供更好可視性



內建派工管理，連動跨品牌的設備，滿足協作聯防、自動化回應 (SOAR) 需求



An astronaut in a white spacesuit stands on the moon's surface. The astronaut's helmet visor reflects the lunar landscape. The background shows the dark sky and the horizon of the moon.

親愛的老師們，感謝您即將使用 FortiSIEM
新世代 SIEM 平台



您決定使用 FortiSIEM 的一小步，
是您校園資訊安全進程的一大步

FORTINET®